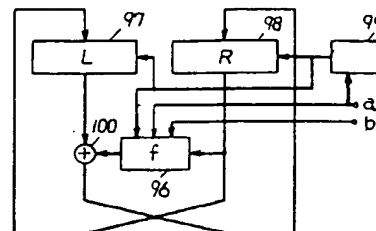


(54) SIGNAL SCRAMBLER AND CIPHERING DEVICE

(11) 5-75596 (A) (43) 26.3.1993 (19) JP
 (21) Appl. No. 3-230147 (22) 10.9.1991
 (71) MATSUSHITA ELECTRIC IND CO LTD (72) NOBORU KATSUTA(3)
 (51) Int. Cl.⁵ H04L9/06, H04L9/14, G09C1/00

PURPOSE: To obtain a ciphering device for secret communication which is capable of processing of plural ciphering algorithms.

CONSTITUTION: Left and right halves of an input signal are inputted to registers 97 and 98 respectively. A signal scrambler 96 repeatedly scrambles a ciphering key and the output of the register 98 at each time of input of a clock pulse. When a preliminarily set number of clock pulses are inputted, a pulse control circuit 99 sends an update signal to registers 97 and 98 to rewrite contents of registers 97 and 98. This operation is performed as the processing in one stage, and the number of pulses in each stage is independently set.



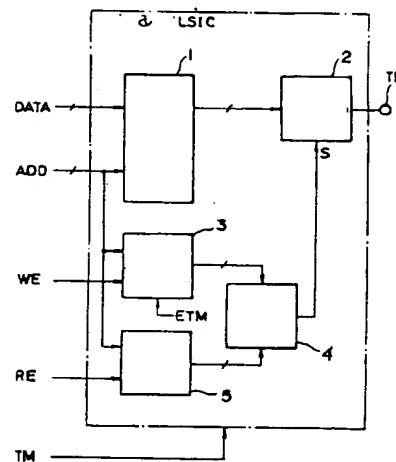
a: clock pulse, b: ciphering key

(54) SECRET KEY PROTECTING SYSTEM AND CIPHER PROCESSING LSIC BY THIS SYSTEM

(11) 5-75597 (A) (43) 26.3.1993 (19) JP
 (21) Appl. No. 3-230580 (22) 10.9.1991
 (71) FUJITSU LTD (72) HIDEAKI TANAKA
 (51) Int. Cl.⁵ H04L9/06, H04L9/14, G09C1/00

PURPOSE: To provide the secret key protecting system and the cipher processing of this system where read/write of a memory part where secret key data is stored can be checked but secret key data cannot be observed from the external.

CONSTITUTION: Data in a memory part 1 where secret key information is stored can be read/written from the external in the test mode. A control part 2 which controls permission/inhibition of external output of read data from the memory part 1, a storage part 3 where all stored information are reset by input of a test mode signal TM and information related to addresses where data is written in the memory part 1 is stored thereafter, and a comparing part 4 which compares stored information of the storage part 3 and information related to the address for data read of the memory part 1 with each other are provided. When the test mode is set and the comparison in the comparing part 4 results in coincidence, the control part 2 permits data output. The memory part 1 and a cipher processing part which generates secret key information are unified and integrated into a cipher processing LSIC to improve the secrecy.



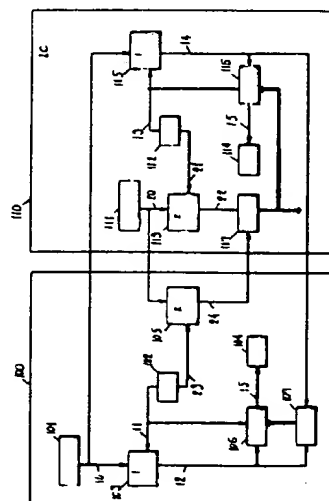
5: gate part, a: cipher processing LSIC

(54) KEY DATA SHARING DEVICE

(11) 5-75598 (A) (43) 26.3.1993 (19) JP
 (21) Appl. No. 3-237699 (22) 18.9.1991
 (71) MATSUSHITA ELECTRIC IND CO LTD (72) YOSHIHIRO MUTO(1)
 (51) Int. Cl.⁵ H04L9/06, H04L9/14, G06F12/14, G06K17/00, G09C1/00

PURPOSE: To eliminate a need of decoding processing to share a session key between communicators while confirming it by communicators of each other.

CONSTITUTION: An information processing terminal 100 and an IC card 110 transmit generated random numbers 10 and 20 to each other and cipher the transmitted random numbers to obtain cipher data 12 and 22. Thereafter, they cipher received random numbers of each other to transmit cipher data 24 and 14. They compare received cipher data and data ciphered by themselves with each other; and in the case of coincidence, they use secret key data and operated cipher data to obtain key data common to them by operation.



101,111: random number generating means, 102,112,104,114: memory, 103,113: first cipher means, 105,113: second cipher means, 106,116: processing means, 107,117: collating means

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平5-75598

(43)公開日 平成5年(1993)3月26日

(51)Int.Cl.⁵

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/06

9/14

G 0 6 F 12/14

3 2 0 C 9293-5B

G 0 6 K 17/00

T 8623-5L

7117-5K

H 0 4 L 9/ 02

Z

審査請求 未請求 請求項の数4(全 5 頁) 最終頁に続く

(21)出願番号

特願平3-237699

(22)出願日

平成3年(1991)9月18日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 武藤 義弘

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 高木 伸哉

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

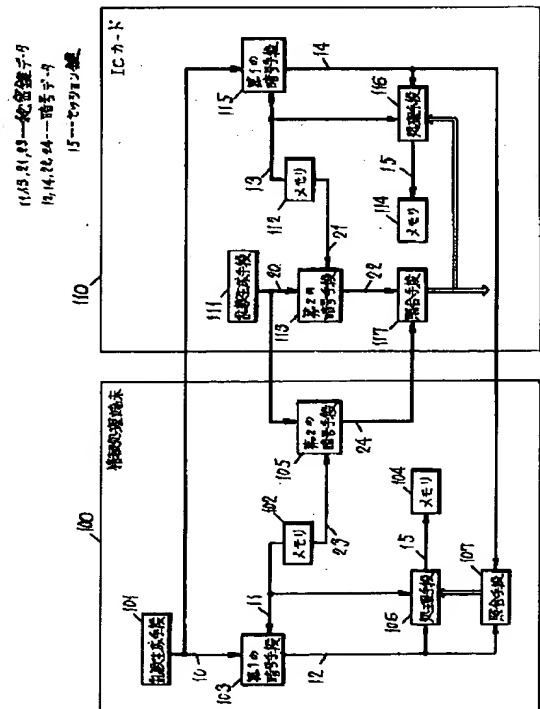
(74)代理人 弁理士 小銀治 明 (外2名)

(54)【発明の名称】 鍵データ共有装置

(57)【要約】

【目的】 復号処理が不要で、通信者間で相互に認証を行いつつ、セッション鍵を通信者間で共有できる鍵データ共有方式を提供する。

【構成】 情報処理端末100とICカード110はそれぞれお互いに、生成した乱数10、乱数20を相手に送信すると同時に、送信した乱数を暗号化して暗号データ12、暗号データ22を得る。お互いにその後、それぞれ受信した相手の乱数を暗号化してその暗号データ24、暗号データ14を送信する。また受信した暗号データと先に自分で暗号したデータを比較し、一致した場合に秘密の鍵データと演算した暗号データとを用いて演算し、お互いの共通鍵データとする。



【特許請求の範囲】

【請求項1】乱数を生成する乱数生成手段と、第1の秘密鍵データと第2の秘密鍵データを格納する第1のメモリと、前記第1の秘密鍵データを用いて演算する第1の暗号手段と、前記第2の秘密鍵データを用いて演算する第2の暗号手段と、前記第1の暗号手段によるデータあるいは前記第2の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段と、前記照合手段の結果によって起動し通信したデータと前記第1の秘密鍵データとを用いて演算する処理手段と、前記処理手段の演算結果を格納する第2のメモリより構成される鍵データ共有装置。

【請求項2】ICカードが接続可能な情報処理端末間で行われる鍵データ共有方式であり、前記ICカードは、少なくとも、第1の秘密鍵データと第2の秘密鍵データを格納する第1のメモリと、前記第1の秘密鍵データを用いて演算する第1の暗号手段と、前記第2の秘密鍵データを用いて演算する第2の暗号手段と、前記第1の暗号手段によるデータあるいは前記第2の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段と、前記照合手段の結果によって起動し通信したデータと前記第1の秘密鍵データとを用いて演算する処理手段とを含み、前記情報処理端末は、乱数を生成する乱数生成手段を含み、鍵データ共有方式における演算をICカードが行うことを特徴とする鍵データ共有装置。

【請求項3】乱数を生成する乱数生成手段と、第1の秘密鍵データと第2の秘密鍵データを格納する第1のメモリと、前記第1の秘密鍵データを用いて演算する第1の暗号手段と、前記第2の秘密鍵データを用いて演算する第2の暗号手段と、前記第1の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段とより構成される通信装置。

【請求項4】乱数を生成する第1の手順と、前記第1の手順の後、前記乱数を送信する第2の手順と、前記第1の手順の後、前記乱数を第1の暗号手段で暗号化し第1の暗号データを得る第3の手順と、前記第3の手順の後、受信した暗号と照合する第4の手順と、受信した乱数を第2の暗号手段で暗号化し第2の暗号データを得る第5の手順と、前記第5の手順の後、第2の暗号データを送信する第6の手順よりなる鍵データ共有方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】暗号通信において、通信を行うもの同士が共通の鍵データ（以後セッション鍵と呼ぶ）を共有するための鍵データ共有方式に関する。

【0002】

【従来の技術】従来、秘密鍵暗号アルゴリズムに基づく暗号処理を実施するために通信者間で使用される鍵は共通の鍵データであり、物理的に安全な方法、たとえば予め装置内に格納して配送するなどの方法で鍵データを共

有していた。またこの秘密鍵データは、通信する相手が多数の場合、相当数の鍵データを予め記憶しておく、あるいは通信に参加している人すべてが共通の一つの鍵データを共有している必要がある。暗号通信においてこの秘密鍵が使用された場合、固定データを暗号化しても固定の暗号化データが計算されるので、通信回線を盗聴されると不正が行われやすく、通常データの暗号化あるいは復号化には直接使用されない。そこで暗号通信には通信毎に変化するセッション鍵を使用する。この秘密鍵データは、セッション鍵を共有するために、鍵データ共有方式で使用される。

【0003】図2にセッション鍵を共有するための従来の鍵データ共有方式の例を示す。ここで情報処理端末210が情報処理端末220との間でセッション鍵を共有する方式について説明する。メモリ213およびメモリ223には、予め共通の秘密鍵データ31が格納されているものとする。

【0004】情報処理端末210において、鍵データ生成手段211は暗号処理を実施するために通信者間で使用されるセッション鍵30を生成する。メモリ213に格納されている秘密鍵データ31で暗号手段212によりセッション鍵30を暗号化し、情報処理端末220に送信する。情報処理端末220は受信した暗号データ32をメモリ223に格納されている秘密鍵データ31で復号化手段222により復号化する。復号化して得られたセッション鍵40は不揮発性のメモリ221などに格納して、情報処理端末210と情報処理端末220との間でデータを共有できる。

【0005】

【発明が解決しようとする課題】従来の鍵データ共有方式においては、復号手段が必須であり、また暗号通信など暗号処理を行う前に、不正防止のために通信相手の認証処理が必要となる。これら多くの処理はICカードなどの演算能力が低い装置にとってはメモリ容量および処理の負担が大きくなる。

【0006】本発明はかかる点に鑑み、復号処理が不要で、通信者間で相互に認証を行いつつ、セッション鍵を通信者間で共有できる鍵データ共有方式を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明は上記目的を達成するために、乱数を生成する乱数生成手段、第1の秘密鍵データと第2の秘密鍵データを格納する第1のメモリと、前記第1の秘密鍵データを用いて演算する第1の暗号手段と、前記第2の秘密鍵データを用いて演算する第2の暗号手段と、前記第1の暗号手段によるデータあるいは前記第2の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段と、前記照合手段の結果によって起動し通信したデータと前記第1の秘密鍵データとを用いて演算する処理手段と、前記処理手段の

演算結果を格納する第2のメモリとを含む情報処理端末間により許容される鍵データ共有方式である。

【0008】

【作用】この方式により許容される鍵データ共有方式は、情報処理端末に格納する秘密の鍵データの数を削減し、また復号処理が不要であるため、メモリ容量および処理を削減することが可能となる。また、相互認証処理を行う都度にランダムな秘密の鍵データを通信者間で共有するため、この共有鍵を使用した安全性の高い暗号化処理が可能となる。

【0009】

【実施例】以下、本発明の一実施例について図面を参照しながら説明する。図1は本発明の実施例による鍵データ共有方式を示した構成図である。100は情報処理端末、110はICカードであり、情報処理端末100とICカード110との間でセッション鍵を共有する方式について説明する。情報処理端末100の秘密鍵データ11と秘密鍵データ23およびICカード110の秘密鍵データ13と秘密鍵データ21は予めシステムを管理しているセンターによって格納されるものである。

【0010】情報処理端末100は、乱数生成手段101により乱数10を生成し、ICカード110に送信する。同時に、第1の暗号手段103によりメモリ102に格納されている秘密鍵データ11を用いて乱数10を暗号化し、暗号データ12を得る。

【0011】ICカード110は、第1の暗号手段115によりメモリ112に格納されている秘密鍵データ13を用いて情報処理端末100から受信した乱数10を暗号化し、暗号データ14を得る。乱数生成手段111により乱数20を生成し、情報処理端末100に送信する。同時に、第2の暗号手段113によりメモリ112に格納されている秘密鍵データ21を用いて乱数20を暗号化し、暗号データ22を得る。

【0012】情報処理端末100は、第2の暗号手段105によりメモリ102に格納されている秘密鍵データ23を用いてICカード110から受信した乱数20を暗号化し、暗号データ24を得る。その後、暗号データ24をICカード110に送信する。

【0013】ICカード110は、照合手段117により暗号データ22と情報処理端末100から受信した暗号データ24を比較する。不一致の場合は、以後の処理は打ち切れ、一致した場合は、暗号データ14を情報処理端末100に送信するとともに、処理手段116により秘密鍵データ13と暗号データ14を用いて演算（例えば排他的論理和）し、この演算結果をセッション鍵としてメモリ114に格納する。

【0014】情報処理端末100は、照合手段107により暗号データ12とICカード110から受信した暗号データ14を比較する。不一致の場合は、以後の処理*

*は打ち切れ、一致した場合は、処理手段106により秘密鍵データ11と暗号データ12を用いて演算（例えば排他的論理和）し、この演算結果をセッション鍵としてメモリ104に格納する。

【0015】センターによって認められた情報処理端末およびICカードであれば、すなわち、情報処理端末100の秘密鍵データ11とICカード110の鍵データ13が同一であり、かつ情報処理端末100の秘密鍵データ23とICカード110の鍵データ21が同一であれば、それぞれの情報処理端末あるいはICカードにおける照合手段による結果は一致し、お互いに認証が行え、かつ共通のセッション鍵が共有できる。

【0016】なお、本実施例では、処理手段106および116における演算に排他的論理和を用いたが、2つのデータの内一方を鍵データ、他方を平文データとして暗号化することも考えられる。また、この演算に用いられる2つのデータは、秘密鍵データとお互いに同じ演算を施したデータとであればどのような組合せでも可能である。

【0017】さらに、本発明の鍵データ共有方式によって共有したセッション鍵を用いて、次の暗号処理に用いる鍵データを交換する事も容易である。例えば、共有したセッション鍵を判定パラメータとして、このパラメータと交換したい鍵を用いて、暗号処理を施し相手に送信する。受信者は受信データを復号処理した後、パラメータを判定し、一致すれば次に使用する鍵データを交換する。

【0018】また、鍵データ共有方式は、高い安全性が要求され、特に情報処理端末100のメモリ102からはデータが読み出せないようにする必要がある。本発明では、ICカード110とは別の第2のICカード（以下セキュリティモジュールと呼ぶ）で前記一連の鍵データ共有方式を実施することが可能である。このセキュリティモジュールは情報処理端末に接続した形で使用する。なお、セキュリティ上セッション鍵を格納するメモリは、不揮発性メモリにするのが望ましい。

【0019】

【発明の効果】以上のように本発明によれば、ICカードに格納する鍵データは2つの秘密鍵だけであり、また処理的にも復号処理は不要となり、メモリ容量は少なくすむ。また、通信者間で相互に認証を行うため、高い安全性のもとで鍵データの共有が可能である。

【図面の簡単な説明】

【図1】本発明の実施例による鍵データ共有方式を示した構成図

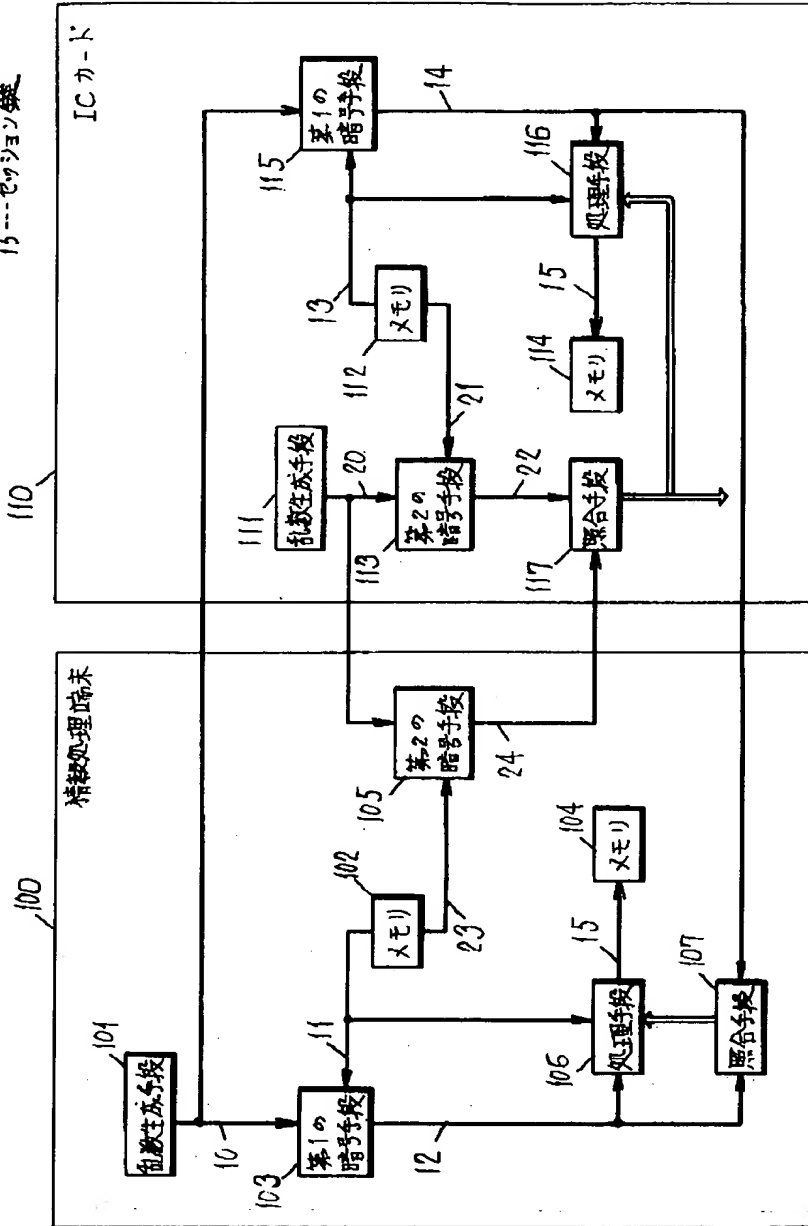
【図2】従来の鍵データ共有方式を示した構成図

【符号の説明】

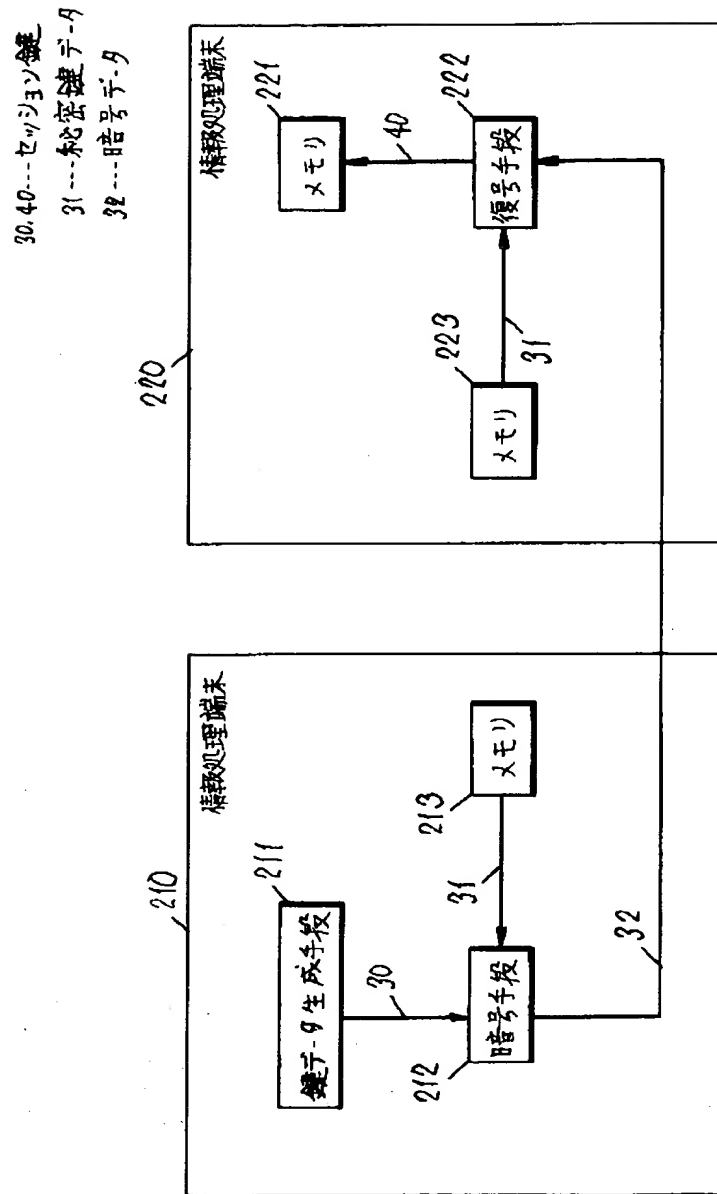
100 情報処理端末
110 ICカード

【図1】

11,13,21,23---秘密鍵データ
12,14,22,24---暗号データ
15---セッション鍵



【図2】



フロントページの続き

(51)Int. Cl.⁵

G 0 9 C 1/00

識別記号

庁内整理番号

9194-5L

F I

技術表示箇所